Amendments to the Specification:

Please replace paragraph [0061] with the following amended paragraph:

[0061] FIG. 6 shows the steps involved in validating the ballot request and generating an electronic ballot. The voting mediator receives the sealed (signed and encrypted) ballot request 53 and decrypts the encrypted ballot request with the mediator's private key to get the signed ballot request 54. The voting mediator validates the voting entity's certificate 55 and authenticates and verifies the integrity of the signed ballot request using the public key within the voting entity's certificate 56. The voting mediator validates the entity's certificate by ensuring that the certificate's validity period has not expired, that the certificate can be traced to a trusted root certificate, that the public key of the certificate issuer validates the signature of the certificate, and that the certificate does not exist on a Certificate Revocation List (CRL) issued by the certificate issuer. If the request is valid, the voting mediator authorizes the ballot request 57 by checking the signing certificate information against the appropriate election database, such as a registered voter roll for the state or municipality and whether or not the voting entity already voted in the target election. The voting entity's certificate information would include for example, the voter's address and precinct number. If the entity's certificate is valid, the mediator must ensure that the ballot request belongs to the entity requesting the ballot. The mediator extracts the public key from the entity's certificate and uses the entity's public key to validate the signature of the signed ballot request. The signature is an encrypted hash of the ballot request. The encryption of the hash was performed by the entity's private key. Once the mediator decrypts the encrypted hash with the public key of the entity, the mediator gets a decrypted hash. The mediator also computes the hash of the ballot request. If the decrypted hash ~~has~~ and the computed hashes are the same, the mediator has validated the ballot request came from the voting entity identified by the entity's certificate. If the request is authorized, the voting mediator creates an electronic ballot 58 consisting of the unique election identification and ballot serial number. The entire ballot is encrypted with the public key of the voting tabulator, which was obtained from the certificate of the voting tabulator 59. The voting mediator places the encrypted electronic ballot and voting tabulator's certificate in a message that is signed with the voting mediator's private key 60. The voting mediator also encrypts the signed information 61 with the public key of the voting entity before sending the signed and encrypted information, which includes the encrypted electronic ballot, to the voting entity 62.